Data Security Breaches:
The Growing Liability Threat
Crafting and Implementing Policies to Prevent and Respond to Inadvertent Disclosures

A Live 90-Minute Teleconference/Webinar with Interactive Q&A

Today’s panel features:
Jonathan T. Rubens, Of Counsel, Bullivant Houser Bailey, San Francisco
Catherine D. Meyer, Counsel, Pillsbury Winthrop Shaw Pittman, Los Angeles
Aaron P. Simpson, Hunton & Williams, New York

Thursday, February 11, 2010
The conference begins at:
1 pm Eastern
12 pm Central
11 am Mountain
10 am Pacific

You can access the audio portion of the conference on the telephone or by using your computer’s speakers.
Please refer to the dial in/ log in instructions emailed to registrations.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click Bookmarks or Pages on the left side of the window.
If no icons are present: Click View, select Navigational Panels, and chose either Bookmarks or Pages.

If you need assistance or to register for the audio portion, please call Strafford customer service at 800-926-7926 ext. 10
For CLE purposes, please let us know how many people are listening at your location by

• closing the notification box
• and typing in the chat box your company name and the number of attendees.
• Then click the blue icon beside the box to send.
DATA SECURITY BREACHES: THE GROWING THREAT

PART I: RECENT STATE LEGISLATION AND CIVIL LITIGATION

Jonathan T. Rubens
Bullivant Houser Bailey PC
San Francisco

Jonathan.rubens@bullivant.com
Key Federal Legislation Addressing Data Security Practices

- Fair Credit Reporting Act of 1970
- Video Privacy Protection Act of 1988
- Electronic Communications Privacy Act of 1986
- Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994
- HIPAA (1996)
- Gramm-Leach-Bliley (1999)
- Fair and Accurate Credit Transactions Act of 2003
- Red Flags Rule (2009)
- Hi-Tech Act (2010)
CA Data Security / Breach Law

• California – where it started
  – Requires data security procedures and practices that are “reasonable” and “appropriate to the nature of the information”. Civil Code Section 1798.81(5)(b)
  – Requires notice following breach. Section 1798.82;
California Data Security / Breach Law

• California: “personal information” means:
  – First name or first initial and last name, in combination with any of:
    • SSN
    • Drivers License No.
    • Credit Card #, Debit Card # along with login and password;
    • Medical Info (added more recently):

  – Notice required following breach regardless of evidence of harm
Massachusetts

- New Mass Law effective March 1, 2010 – MGL Ch 93H -
- Requires notice following breach to consumers and state:
  - Notice required, from a person that owns or stores information about a resident, to the owner or licensor of the information, when the person knows or has reason to know that the information was acquired or used by an unauthorized person or for an unauthorized purpose;
  - From the owner or licensor, to the attorney general, the director of consumer affairs and business regulation and to the resident.

(Ch 93H section 3)
Massachusetts

• Defines Personal Information as:
  – A resident’s first name or first initial, plus last name, with one or more of
    • SSN
    • DL or State ID Card number
    • CC #, Debit Card #, financial account #, with or without any required security or access code, PIN, or password

• Applies to any person, corporation, or other legal entity that owns, licenses, maintains, or stores the personal information of a resident of Massachusetts (whether or not such person is present in Massachusetts).
Massachusetts

- Statute directs dept. of consumer affairs to adopt regs:
  - to “safeguard the personal information of residents of the Commonwealth”
  - to be “consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated” (Section 2(a))
  - to “insure the security and confidentiality of customer information in a manner fully consistent with industry standards”

(Ch 93H Section 2(a))
Massachusetts - Regulations

• 201 Mass Code Regs. 17.00 et seq. impose “minimum standards to safeguard personal information in both paper and electronic records” on companies that collect, store or transmit personal information concerning Massachusetts residents.

• Regs require development of a comprehensive “written information security program” (WISP) for records with personal information
Mass Regs

• WISP must include:
  – Designation of a employee in charge of WISP
  – Identifying internal and external risks to security of records containing PI;
  – Employee policies and discipline;
  – Preventing terminated employee access to PI;
  – Service provider oversight;
  – Data storage;
  – Monitoring, Updating;
  – Documenting response to breach.
Mass Regs

• WISP must include a security plan that addresses:
  – *Encryption of all personal information* transmitted across public networks or stored on laptops, portable devices;
  – Secure user authentication protocols;
  – Secure access control measures;
  – Monitoring for unauthorized system access;
  – “Reasonably up-to-date firewall protection and OS system patches” for a network connected to the Internet;
  – “Reasonably up-to-date” system security agent software that includes malware protection and “reasonably up-to-date patches and virus definitions”;
  – Employee training on the security system and protection of PI;
Massachusetts

- Compliance deadline: Mach 1, 2010
- Attorney general may bring action “to remedy violations of this Chapter and for other relief that may be appropriate.”
- Attorney General may seek injunctive relief against the person involved in an unauthorized act or practice at issue.
- Court may impose $5,000 civil penalty for each violation
Nevada

• Businesses must encrypt personal information
  – on data storage or mobile devices moved beyond the “physical or logical controls” of the business; or
  – When data is transferred “through an electronic non-voice transmission other than a facsimile” outside the secure system of the business

• Business that accept payment cards must comply with PCI DSS

• Defines acceptable levels of encryption
Minnesota

- Prohibits retention of security codes and other credit card data after processing transactions
- Requires merchants to reimburse credit-card issuing financial institutions for costs incurred following a data breach
- Creates private right of action for financial institutions following noncompliance by merchants
- Minn. Stat. 365E.64.
Other Jurisdictions; Potential Laws

• Data breach notification statutes now on the books in 45 states

• D.C., Puerto Rico, US V.I.

• Federal legislation introduced in both the House and the Senate in 2009, based on state breach notification statutes
FTC Enforcement

• FTC’s Authority to Regulate Data Security Practices
  • Broad power under §5 of FTC Act to regulate "unfair or deceptive acts or practices in or affecting commerce"
  • Enforcement Responsibility for Specific Statutes
    • COPPA TCFAPA
    • CAN-SPAM FCRA
    • GLB FACTA / RED FLAGS RULE
FTC Enforcement - ChoicePoint

• Data broker ChoicePoint paid $10 million in civil penalties, $5 million for consumer redress
• Failed to ensure that customers had a legitimate purpose for personal info (e.g. SSN’s)
• Privacy policy: “we comply w/ FCRA; red flags rule”
• See also Reed Elsevier and Seseint (both settle charges that they “failed to provide reasonable and appropriate security for sensitive consumer information”; involved inadequate procedures for dealing with user credentials)
FTC Enforcement - CVS

- **CVS** pays $2.25 million to settle FTC charges for disposing in open dumpsters medication-related bottles, documents, employment applications, SSN’s
- FTC charged that security practices were “unfair”

- See also DSW, Inc., Cardsystems Solutions
FTC Enforcement - Lifeisgood

• Online apparel retailer Lifeisgood.com privacy policy said data is stored in a “secure file”
• FTC alleged “unnecessarily risked credit card info by storing it indefinitely”
• Failed to adequately assess security risk, employ available, low-cost procedures
FTC Enforcement – BJ’s Wholesale, Inc.

- FTC alleged that certain practices “taken together” did not provide reasonable security
- BJ’s failed to encrypt consumer info during transmission
- Created “unnecessary risk” to credit card info by storing it for “up to 30 days
- Info could be accessed using default id’s and passwords
- Failed to use “readily available” security measures
Failure or Delay of Notification

- First state case under the HI-Tech Act
- Alleges massive data breach by HealthNet in May 2009 exposed medical information of 1.5 million enrollees, close to 450,000 in CT
- HealthNet did not notify until November, 2009
Bank recovery of costs associated with merchant data breach

- Cumis Insurance Society, Inc., et al. v. BJ’s Wholesale Club, (MA, Dec., 2009)(affirming dismissal of claims of credit unions and insurance companies based on alleged status as third party beneficiaries of contracts between BJ’s and acquiring bank, contract between bank and Visa).

Consumer recovery of damages from actual or threatened identity theft

- **Shames-Yeakel v. Citizens Financial Bank** (N.D. ILL, August, 2009) (allowing negligence claim where bank not using sufficient identity theft prevention techniques; bank had sued plaintiff first for amounts stolen from HELOC)
- **Rowe v. UniCare Life & Health Ins. Co.**, (N.D. Ill)
- **Pisciotta v. Old Nat’l Bancorp** (7th Cir. 2007)(allowing individual case to proceed on the basis of potential exposure to identity theft following large data breach)
No Consumer recovery of damages from potential identity theft following breach

• **Amburgy v. Express Scripts, Inc.**, , Case No. 4:09CV705, (Eastern District MO November 23, 2009).


Class Actions

• Heartland Payment Systems, Inc.
  • Massive Data Security Breach ( >100 million payment card records)
  • 16 separate class action complaints, alleging hundreds of millions of dollars in damages have been consolidated
  • Already spent $13 million on breach related costs
DATA SECURITY BREACHES: THE GROWING THREAT

PART II: PREPARING FOR THE INEVITABLE

February 11, 2010

Catherine D. Meyer
Pillsbury Winthrop Shaw Pittman LLP
Disclaimer

THIS PRESENTATION DOES NOT CONSTITUTE, AND SHOULD NOT BE RELIED UPON AS, LEGAL ADVICE. YOU ARE ENCOURAGED TO CONSULT YOUR OWN COUNSEL REGARDING THE APPLICATION OF ANY OF THESE OR OTHER LAWS TO YOUR COMPANY, TO YOUR CLIENT, OR TO YOUR SPECIFIC CIRCUMSTANCES. THANK YOU.
Why do we care?

Ripped from the Headlines:

Hacked: ING Belgium, Dexia and HSBC France websites

Electronic voting machines easily hacked, researchers say

Veteran’s Administration loses confidential information of 29 million veterans

Backup tapes lost containing thousands of customer records

Retailers hacked – thousands of credit card numbers stolen

Healthcare organization loses hard drive containing patient records

Universities hacked - student and alumni data stolen

Credit card numbers stolen via wireless insecurities

Three alleged hackers indicted in large identity – theft case
2010 Data Breaches
Open Security Foundation

http://datalossdb.org/index/latest

- Eugene School District (Hack)
- Suffolk County National Bank (Hack)
- Kaiser Permanente Northern CA (Stolen Drive)
- City of Oakridge Oregon (Postal Mail- SSNs – Internal Accidental)
- Goodwill Industries of Greater Grand Rapids (Stolen Tape)
- University of Missouri (Postal Mail- Visible SSNs-Internal Accidental)
- City of Columbus, Ohio (Unknown- exposed SSNs)
- Ladbrokes (UK) (Unknown-Internal) (Gambling records offered for sale)
- Methodist Hospital (Stolen laptop)
- PF Change’s Bistro (Stolen computer)
- University of California San Francisco (Stolen laptop)
- Ontario Can. Teachers Ins. Plan (Stolen laptop)
- National Archives (Lost disk drive)
- State of Alaska – PriceWaterhouseCoopers (Unknown)
- Ameriquest Mortgage (Internal fraud)
- Rabjohns Financial Group (Internal Accidental-Document disposal)
- Iowa Racing and Gaming Comm’n (Hack)
- Humboldt State Univ. (Virus)
- Columbia Univ. (Stolen Laptop)

Over 470,000 records
And that just gets us through January…
Where and how do breaches occur?

2009 Data Breach Investigations Report

- 74% from external sources
- 20% from internal sources

- 64% from hacking
- 22% involved privilege misuse
- 67% were aided by significant errors

- 17% of attacks were rated “highly difficult” but accounted for 95% of total records
Does it matter if your customers said...

- 2008 Ponemon Institute *Consumer’s Report Card on Data Breach Notification* results
  - 57% of notice letter recipients had lost trust and confidence in the notifying organization
  - 31% of recipients had terminated their relationship with notifying organization
  - 63% complained the notice letters offered no direction on protecting their personal information
- Take-away: Look at the cost of giving timely, helpful notification, credit protection services and resources for self-help against cost of customer acquisition
- Full study available at www.idexpertscorp.com
Would you care if….

- A trusted employee pasted confidential acquisition information into a webmail message and sent it to your competitor?

- An employee downloaded hacker tools to their work computer with the intention of stealing your customer's private data?

- An employee posted your confidential executive communications or financial data on www.internalmemos.com or some other internet posting site like Yahoo Finance?

- An employee is using a P2P client and is inadvertently exposing your proprietary information to millions of other P2P users?
What if your vendor …..

- Used your customer information to market their own products ….. or your competitors’?
- Had no security for protecting your customers’ credit card numbers?
- Gave hackers access through your website to your customer data, your financial data, your trade secrets, your employee information?
- Promised strong security measures, but never used them?
- Exposed your data in a security breach costing you millions?
Data Breach Costs -100,000 records

Darwin National Assurance Company, which offers a technology insurance product called Tech/404, has a calculator on its website to help you estimate what a a loss will cost. (Available at http://www.tech-404.com/calculator.html)

According to this calculator, a loss with 100,000 affected records will cost, on average:

- **Investigation:**
  - Consultants: $483,000
  - Attorneys: $489,720

- **Notification:**
  - Customer Notification: $890,400
  - Call Center Support: $630,000
  - Crisis/Media Management: $422,520

- **Regulatory**
  - Credit Monitoring (2 years): $4,048,800
  - Investigation Defense: $1,497,720
  - State/Federal Fines/Fees: $3,176,880

**Total Cost:** $11,639,040
Reviewing the risks

The risks are more than just immediate monetary impact:

- Financial Loss
- Regulatory Fines
- Litigation
- Reputation Loss
- Loss of System Availability
- Lost Productivity
- Loss of Intellectual Property
Managing and Mitigating Legal Risk

Know the Laws/Regulations and Track Changes

- Hundreds of laws and regulations in the US alone
- Internationally--there are even more
- Need capable people
- Make sure relevant information is provided to appropriate people in the company
Managing and Mitigating Legal Risk

Similar to Managing any Compliance/Legal Risk

- Be able and willing to adjust practices and policies
- Watch for trends in regulatory actions and litigation
- Ensure legal is involved in material changes and contracts
  - New products or services
  - Expansion or contraction of company, products, services
  - Sales or purchases of assets, companies
  - Offshore operation
  - Special marketing arrangements
Managing and Mitigating Legal Risk

Significant Legal Risk Areas Today

- Failure to Protect Customer Database - arguably the company's most important asset
  - Security breaches
  - Oversight of how third parties handle your data and abide by contractual commitments
- Employee data, especially where used to discipline or terminate
- Identity theft causing consumer fraud or loss
- Protection of IP in age of increased sharing
- Failure to keep Privacy Promises
  - What is the company committing to do in terms of sharing, etc.?
  - Collection of information or monitoring/recording information in an illegal manner (albeit it, unintentionally)
  - Data sharing and mining, especially for marketing purposes
Managing and Mitigating Legal Risk

Traditional Legal Risk Mitigation Strategies

- Appropriate polices, procedures and practices
  - Update as needed and review frequently to make sure they work
  - Audit or independent reviews
- Clear identification of responsible employees/officers
- Training of employees and, if needed, third parties
- Audit or oversight of third parties handling or having access to your data
- Stay current on information and trends; involvement in appropriate associations
Responding to a Data Security Breach
-It’s not “If” it’s “When”
What Works?

- Prompt Responsiveness
- Right Group of People
  - Legal, Risk Management, Operations, Senior Management
- Thorough Review of Data Involved
- Notification When Appropriate
What Doesn’t?

- Delay
- Disorganization
- Concealment
Be Prepared: Your Best Defense

Review:
Privacy policies to ensure compliance

Test & Train:
Verify security systems and backup/archives periodically

Written Plan:
Contact Information:
Team members - Law enforcement - Regulators
Basic Response Documents:
Notice letter – FAQs - Press release
Data Loss Prevention

- Monitor
  - Web
  - Email
  - Telnet
  - Chat
  - IM
  - Webmail
  - P2P
  - FTP
  - Attachments
  - And more...
- Analyze
  - Determine Type
  - Analyze Content
  - Interpret Context
  - Identity Match
  - Over 50 Pre-Defined Categories
  - Custom Search Parameters (CSPs)
- Capture
  - URL Database
- Manage & Report
  - Alert, Notify
  - Identify Inappropriate URLs

Internet Traffic and Stored Data
Linguistic Intelligence
Store Events
Information Delivery

Updates to URL Database
Security Awareness Training
- It is Not Just Hackers

- Employees need to be trained and re-trained on the importance of maintaining security.
- Training needs to address social engineering techniques that are typically very effective at convincing employees to provide sensitive data.
  - Calls from help-desk
  - Calls to help-desk
  - Phishing attacks
  - Physical compromise
  - USB devices

Sample Security Awareness materials are available at:
- http://cyberexchange.isc2.org
Incident Response Plan

Regulators may require written plan

- Massachusetts
- Identity Theft Red Flag Rule
- GLBA
Incident Response Plan: Overview

- **Response Program Objectives**
- **Identify Team Members**
  - Contact information
  - Identify, vet and get approvals for outside experts and vendors
- **Incident Action plan**
  - Alarms
  - Reporting up
  - Centralized mechanism for reports
- **Incident Response Stages**
  - Preparation
  - Early Team Meeting
  - Training
  - Investigation
  - Containment Assessment
  - Notification
  - Ownership and Management Oversight
Incident Response Plan: Internal Team Members

- Law Enforcement
- Executive Team
- Information Technology Information Security
- Human Resources
- Public Relations
- Risk Management Compliance
- Legal
- Outside Legal
- Card Associations
- Forensics
Incident Response Plan: External Team Members

- Law Enforcement
- Information Technology Information Security
- Outside Legal
- Executive Team
- Card Associations
- Human Resources
- Risk Management Compliance
- Public Relations
- Forensics

24 | Data Security Breaches
Incident Response Plan: Preparation

- Basic Response Documentation
  - Notice Letter
  - Card Association Notice
  - Regulator Notice
  - FAQs
  - Agency Notifications
  - Press release templates

- Credit Monitoring Contacts

- Call Center Contacts

- Annual drills
SECURITY BREACH PREPARATION AND RESPONSE ACTION PLAN

Five Steps to Prepare for and Effectively Manage a Security Breach

1. Form an Incident Response Team.
   You should have a team in place and notify them immediately when a security breach occurs. The team should include employees and officials of your company, as well as enforcement officials and regulators. On the back of this plan is a form for you to complete with the names and contact information of the key players of the team.

2. Prepare for a Breach.
   Your team should be ready to anticipate problems and potential litigation through pre-planning. This includes (a) having a basic response plan ready at all times, which includes a crisis response team, a crisis response coordinator, and a written plan, (b) investigating all breaches, and (c) reviewing all response plans and correcting them.

3. Engage in Discovery and Investigation.
   Once a breach occurs, you will need to notify and organize the response team. You may need to engage a forensic team to assess evidence of the event, determine how to handle the investigation, and consult with your insurance carriers. You will need to interview all witnesses, document the evidence, and review all response plans. It is important to ensure that the strong points of your response plan are in alignment.

4. Issue Notification to Customers.
   Depending on the state, you may need to provide notice to customers that a security breach occurred. Additional notice to regulatory agencies may also be required, as well as notice to criminal reporting agencies. The notification should include a description of the breach and the steps taken to resolve it.

5. Conduct a Post-incident Review.
   After the breach, the team should review the response plan and consider all actions taken. The team should also review all vendor contracts, policies, and documentation, and create a written response plan. In addition, the team should consider conducting an independent review of the breach to determine how to improve its response plan.

Overview

The issue of a data security breach affecting a company is a question of “when,” not “if.” Pillsbury routinely helps clients to develop and implement effective breach response policies and procedures. This action plan is meant to help you prepare for and respond to a security breach.

Privacy & Data Protection

SECURITY BREACH PREVENTION AND RESPONSE ACTION PLAN

Seven Questions to Address in a Consumer Notification of a Security Breach

1. What information was involved?
2. Was data improperly accessed, acquired or disclosed?
3. Likelihood of release?
4. Was data protected? (e.g., passwords, encryption, shredding)
5. Where are individuals usually?
6. Are credit cards involved?
7. Do we have contact information (mailing address) for all involved?

Your Security Breach Response Team

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For additional information contact:

Dorothy H. Tuckey-Peterson | 212-865-7286 | dotuckey-peterson@ pillsburylaw.com
Catherine B. Meyer | 212-488-7162 | cmeyer@ pillsburylaw.com
Wayne C. Matti | 212-488-1774 | wayne.matti@ pillsburylaw.com
John J. Michel | 212-488-1774 | john.michel@ pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP | 1400 Pennsylvania Ave NW, Washington, DC 20004 | Tel: 202-966-5000

ATTORNEY ADVERTISING. Results depend on a number of factors unique to each matter. Past results do not guarantee a similar outcome.

Pillsbury Winthrop Shaw Pittman LLP | 1400 Pennsylvania Ave NW, Washington, DC 20004 | Tel: 202-966-5000

www.pillsburylaw.com

Data Security Breaches
Catherine D. Meyer, Counsel
Pillsbury Winthrop Shaw Pittman, LLP
725 South Figueroa Street
Suite 2800
Los Angeles, CA 90017-5406

Tel: 213.488.7362
Fax: 213.226.4160

catherine.meyer@pillsburylaw.com
Data Security Breaches: The Growing Liability Threat

Aaron P. Simpson
Hunton & Williams LLP
(212) 309-1126
asimpson@hunton.com
huntonprivacyblog.com

February 11, 2010
Our Firm

• Founded in 1901, Hunton & Williams is one of the nation’s leading law firms with nearly 1000 attorneys in 18 offices, serving clients in over 100 countries

• 20 privacy professionals in the U.S., EU and Asia

• Our privacy clients include:
  – GE
  – Polo Ralph Lauren
  – General Dynamics
  – Estee Lauder
  – Wal-Mart
  – TJX
  – MasterCard Worldwide
  – Time Inc.
  – Macmillan
  – Philips Electronics

• The Center for Information Policy Leadership at Hunton & Williams

• www.huntonprivacyblog.com
Immediate Steps Following a Breach

- Conduct an investigation to determine the facts
  - What happened?
  - Who was affected?
  - What data?
  - What systems?
- Consider whether the investigation should be conducted by internal or external parties
- Does the event trigger notification to individuals under the state or federal breach notification laws?
  - Was the PI “acquired” or “accessed” by an “unauthorized” person?
- Consider your obligations
  - Are you the data owner or licensee?
  - Are you a service provider?
Law Enforcement

- When should you involve law enforcement?
  - Local law enforcement
  - Federal agents
  - Foreign law enforcement
When to Notify

- Timing requirements for notice letters
  - Most states require that an entity notify affected individuals “in the most expedient time possible and without unreasonable delay”
  - A few states require notice to individuals within 45 days
  - Two states have guidance documents that suggest that notification should be sent to affected individuals within 10 days
  - Puerto Rico requires notice to the state agency within 10 days
  - HITECH requires notification within 60 days of discovery
Timing Exceptions

- Exceptions to immediate notification
  - Investigation and restoration
    - Take measures necessary to determine the scope of the breach and restore the reasonable integrity of the system
  - Law enforcement delay
- If you rely on exceptions, document the basis for delay
Preparing the Notification Letter

- Letters must be written with numerous readers in mind:
  - Impacted individuals
  - Regulators
  - Plaintiffs’ lawyers
  - Public at large
  - Media
  - Employees

- If you notify in one jurisdiction, notify in all jurisdictions (including foreign)
  - Overseas notification standards
Notice to Affected Individuals

- Plain language notice
- Describe:
  - The event (but not in Massachusetts)
  - Personal information involved
  - Steps taken to protect against further unauthorized acquisition
  - How the company will assist affected individuals
  - Guidance on how individuals can protect themselves from identity theft or account fraud
  - State-specific information
    - Be careful to review all state content requirements and avoid cutting corners
Expected Offerings

- Notification letters to affected individuals generally contain a number of standard “offerings”
  - Instructions to close bank accounts or cancel credit cards, if necessary
  - Availability of free credit reports
  - Offer of an identity protection solution such as credit monitoring
  - Ability to place a fraud alert or security freeze in credit file
  - Reference to the FTC website
- A number of statutes now require these elements
Pre-mailing Plan

- Need substantial pre-mailing plan of action
  - Prepare press release or holding statement
  - Set up your call center
    - Prepare scripts/FAQs
    - Conduct agent training
    - Monitor initial calls
  - Draft website materials
  - Set up identity protection arrangement
  - Consider investor relations
Other Notification Requirements

- Regulatory agencies
  - FTC, HHS and other relevant federal regulators
    - Requirement for financial institutions and HIPAA covered entities
  - State agencies
  - Non-U.S. regulators

- Payment card brands
  - Check contracts early
  - Notify if necessary
  - Expect rigorous follow up

- Consumer reporting agencies
Increased Regulator Interest

- New Hampshire and Maryland post notices they receive
  - These notices provide a heads-up to other regulators
- State AGs are showing interest
  - They read the letters!
  - More investigations and enforcement actions
- Uptick in FTC investigations and enforcement
  - More access letters
  - More settlements
- Now HHS has joined the party
Avoiding Private Lawsuits

- Understand the scope of the breach before announcing it
- Finalize plan of action in advance of the announcement
- Don’t skimp on use of expert third parties (forensic investigators, lawyers, fraud specialists, PR firms)
- Be transparent, generous and helpful
  - To affected individuals and to the regulators
- Try to avoid thinking like a litigator
Recent FTC Enforcement Actions

- The FTC is the federal agency that enforces against companies that have suffered breaches.
- The FTC's enforcement authority stems from Section 5 of the FTC Act, which prohibits “unfair” or “deceptive” trade practices.
- FTC enforcement actions began with the “deception” prong and have now evolved to use of the “unfairness” principle.

- Petco
- Tower Records
- Barnes & Noble.com
- Guess.com, Inc.
- ChoicePoint
- DSW
- BJ’s Wholesale Club
- TJX
- Reid Elsevier and Seisint

- FTC’s Division of Privacy and Identity Protection
- Enforcement trends
Lessons Learned

- Reputation is everything
- Have an incident response plan and team in place
  - Prevention is the primary goal, but proactive planning can minimize impact if breach occurs
- Involve senior management in data security
- Attacks are more sophisticated than ever
- Re-evaluate security systems and policies on an ongoing basis
- Integrate the concern for information security as a core value and increase employee awareness
Stimulus Package Includes Breach Notice Obligations and Substantial Changes to HIPAA

Provisions of the economic stimulus legislation (known as the American Recovery and Reinvestment Act ("ARRA")), recently passed by the U.S. House of Representatives, require certain entities to notify affected individuals, government agencies and the media of breaches of "unsecured protected health information." Additional provisions substantially revise regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). While these provisions are specifically limited to the context of health data, they have far-reaching implications for businesses across industry that manage personal information. Read more...

TAGS: ARRA, Articles, Breach, HIPAA, Stimulus legislation
Questions?

Aaron P. Simpson
Privacy and Information Management Practice
Hunton & Williams LLP
(212) 309-1126
asimpson@hunton.com
www.huntonprivacyblog.com